2200 Mission College Blvd.
Santa Clara, CA 95054-1549
USA
http://www.intel.com/healthcare

Internet Based Secure Health Data Exchange Testimony for the HIT Standards Committee

*By **Garry Binder**, Senior Architect, Chronic Disease Management Group*
*& **Eric Dishman**, Intel Fellow, Director Health Innovation and Policy*
Intel Corporation

Date: November 23, 2010

Contents

Introduction: A Global Challenge Before Us 3

Intel’s Healthcare and Data Exchange Experiences 4

Standards Used and Intel Recommendations 6

Additional Questions / Answers 12

Summary: Overcoming the Perception Gap 16

Introduction: A Global Challenge Before Us

On behalf of Intel Corporation, we are honored to submit this testimony to the HIT Standards Committee with our recommendations for standards and technologies to reliably and securely share data between healthcare providers. We are very supportive of the efforts of the Office of the National Coordinator (ONC) to help drive widespread adoption and meaningful use of electronic health records. And we are particularly pleased to see the emphasis on helping small and medium-sized healthcare practices adopt health IT through practical, simple guides to the secure exchange of health data.

Given the worldwide demographic and economic realities of rising healthcare costs, a dwindling medical workforce, and increasingly complex, co-morbidity patients to treat, we believe the build-out of local-to-national healthcare information exchanges is essential. Standard & Poor's recent report[i], "Global Aging 2010: An Irreversible Truth," provides a sobering glimpse of the fiscal challenges we face in the U.S. and abroad; we simply cannot afford to deliver healthcare as we have in the past. We need a 21st century health information infrastructure—that enables care coordination, personalized medicine, and community-based support—not only to improve access and quality of care for all Americans, but also to maintain our viability and competitiveness in a global economy.

To that end, based on Intel's experiences worldwide with healthcare and other industries, we believe that secure exchange of healthcare data amongst healthcare providers via the internet is a crucial first step in a long journey to invent a new healthcare system for our nation. In the following pages, we will unpack three simple beliefs:

1) That secure data exchange between healthcare providers (of any size) is doable and achievable today;

2) That several standards and tools are available (e.g., PKI for digital signatures, SMTP for transport, AES for encryption) and should be flexibly deployed depending on the size, needs, and use cases of particular providers;

3) That perhaps the biggest challenge ONC can address is overcoming the perception gap that health data security is somehow unattainable or unaffordable for small physician practices and other healthcare entities who have never done this before.

Intel's Healthcare and Data Exchange Experiences

While Intel is not a healthcare company per se, we are committed in so many ways to healthcare innovation. Our social scientists have spent the past decade studying more than 250 healthcare facilities in 20 different countries—from small physician practices to large hospital campuses to long term care neighborhoods—to help understand workflow challenges, unmet needs, and health IT usage models by an array of medical professionals and patients. Our business development managers have worked with hundreds of healthcare customers around the planet to help them find health information technologies that can meet their needs.

And our technologists and architects have advised and led health IT and standards efforts—creating what we call "solution blueprints"—for healthcare entities in many parts of the world. For example, Intel architects helped the UK with their National Health Information Backbone ("Spine") and their N3 Architecture. We have worked with similar regional and national health exchange efforts in Canada (with Health Infoways) and China (with their RHIN requirements) amongst many others. We are actively supporting NHIN Direct in the U.S. and became a non-voting technical advisor to the recently formed Open Data Center Alliance to help make the vision of Cloud Computing a reality for healthcare and other industries.

More specific to the topic of today's testimony, Intel's Digital Health Group has worked with dozens of healthcare providers to help them manage the secure exchange of Personal Health Information with other providers, including securely sending data to and from telehealth solutions in the home. And through the Continua Health Alliance, Intel originally chaired the team to work with industry partners (including Roche, NHS, Partners Healthcare, IBM) to develop the HL7 Personal Health Monitoring Spec which governs the secure transmission of personal healthcare data between two points, including healthcare providers. This work has recently been publicly demonstrated, with data sent to the NHS clinical spine, to Greenway EHR systems at HIMSS, and to Partners Healthcare EHR.

Intel has engaged in these healthcare-specific efforts by drawing upon our rich history of developing and utilizing B2B (Business-to-Business) communications standards and technology. Intel led the RosettaNet standards effort in the early years, and has contributed on many occasions to EDI standards. Intel also has considerable experience with AS1, AS2 and AS3 (Applicability Statements) for securely transmitting data over the Internet. It is based on these experiences and Intel's less auspicious endeavors using FTP, HTTP and other protocols to exchange data with our own customers and vast supply chain worldwide, that we submit this testimony to the HIT Standards Committee today.

Standards Used and Intel Recommendations

Authentication of End Points and Message Integrity

Arguably the most important aspect of health data delivery is the assurance that the heath care data has come from the claimed source and hasn't been modified. While confidentiality breaches and site outages often make the front page of the morning paper, failure to accurately authenticate the originating data source and message has the potential to do *far more physical harm* than a confidentiality breach or service interruption as scripts or other information could be changed or forged. It is imperative that the best techniques and technologies be used to authenticate the source of the heath care data.

While many modern implementations provide authenticity and message integrity concurrently, some implementations provide one without the other. Such solutions provide a message digest capability in combination with a symmetric encryption algorithm. When the message source cannot be positively identified, proofs of integrity are not relevant. Implementations which provide integrity checks but not authenticity controls should be avoided.

It is Intel’s perspective that PKI based digital signatures provide the most accessible and time tested technology attesting to the authenticity of the sender and message. It is our experience however, that some implementations can reduce the assurance provided by these algorithms. We have seen two integration and implementation behaviors that weaken a strong authentication scheme.

First, some implementations verify and strip off the signature information prior to the payload reaching its destination. Careful downstream implementations *can* reduce the risk that the true identity of the sender is unknown. However, there is no substitute for true end-to-end integrity and authentication, a guarantee that the system has not added or changed primary source data. Systems should retain these signatures with the original payload until it has reached the point of display or processing.

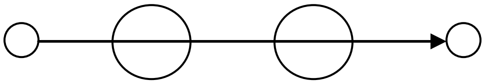

Figure 1: **End-to-End Digital Signatures**

With a strong message authentication and integrity strategy, authentication of the Internet end point is not necessary. A message with a verified digital signature is valid regardless of the mechanism by which it was submitted for delivery. This allows operational reprocessing of messages as needed.

Second, key sharing can dilute the assurance provided by a digital signature. For example, a system (such as an EMR) may have one key that is used to sign outbound messages but hundreds of clinicians will use this EMR to implicitly sign messages with this key. In this contrived example, the strength of the digital signature is limited by the implementation and security policies configured for the EMR. Care should be taken to limit the use of a particular key to the smallest group of users or systems that is practical.

Key Management

Establishing and maintaining the infrastructure to support this strong authentication without impacting the adoption or usability of the solution has always been the most challenging aspect of implementing a PKI based data transfer capability. A conflict exists between truly identifying a person or organization and making it simple to complete this process.

While there is inherent complexity in establishing a digital identity for the first time, once it has been established, renewal can be streamlined relying on a current valid digital identity. A manual auditing function can be put in place to assure that the renewal process is indeed resulting in valid digital identities.

Using Domain Name System (DNS) to distribute digital identities will alleviate some of the difficulties common to Key Management. But, large scale testing should be done to determine the best use of domain hierarchies to ensure that this use scales without impacting ‘normal’ DNS operations.

Encryption

Intel believes that hardware and software should work together to protect the confidentiality of data, both in transit and at rest. For the in-transit part of the equation, Intel recommends link-encryption and for the at-rest portion, full disk encryption.

Link-encryption is the recommended solution when data is sent over unsecured channels. Link-encryption hides routing information while data is on these links and provides message confidentiality. While this does increase the computational load on servers involved in the transaction, modern processors from multiple vendors have the ability to perform many of the needed cryptographic operations directly in silicon. This results in very significant performance gains over the systems without this capability. For medium and large organization this can result in significant reductions in infrastructure complexity and cost.

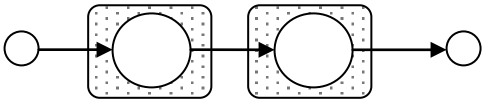

Figure 2: **Link-Encryption**

Link-encryption and full-disk encryption may not, in every case, satisfy the confidentiality requirements of a particular solution. In these cases end-to-end encryption and additional file or folder encryption can be added.

Whether used for link, end-to-end, or data-at-rest protection, the encryption algorithm must be a strong standard algorithm such as AES.

SMTP, SOAP and REST

Both SOAP and REST transport standards are identified widely as incorporating a certain level of complexity. This complexity arises from the flexibility of these solutions and the newness of these solutions when applied in a hostile environment such as the Internet.

A RESTful architecture provides some of the simplest implementations of web services and as a result is very popular among developers and systems integrators. The primary risks of RESTful implementation have to do with PHI or PII getting logged in an unencrypted form in a browser cache, back end server log or other cacheable object. This happens because this data is included as part of the query string (URI) by definition. An analysis of log information could allow an individual to infer more information than is actually provided.

While all or part of the query string can be encrypted and other mitigations can be devised to eliminate the risk of data disclosure it is best to significantly limit or avoid the use of RESTful services for highly sensitive data. At a minimum, organizations can fall back on a set of configuration procedures and periodic audit procedures to ensure that all systems within their control are free of accidental PII / PHI disclosure.

SOAP based web services do not have the same disclosure risks that RESTful services have and in that regard, make a far better choice for the exchange and transmission of health data. For organizations with a larger IT staff SOAP-based web services are clearly a desirable implementation path as it provides real-time delivery of data and the ability to respond on the same connection with an acknowledgement. However the luxury of this type of implementation is beyond the reach of many smaller organizations and individuals. The integration and protection of an externally facing SOAP -based web service capability can be prohibitively costly and complex for some.

SMTP provides the most ubiquitous and time tested transport protocol of the group. It also serves as both a transport of human readable material and a transport for messaging which can be machine parsed, read and imported into a patient record.

Other standards such as AS1 (Applicability Statement 1 – RFC 3335) have been widely used to move EDI data in a secure fashion using existing SMTP infrastructures. AS1 is used in many industries including high-tech, shipping and logistics to send very sensitive information via the SMTP infrastructure. This fact provides field proof that this concept is valid and should serve as a reference for future health data standards.

RFC 2487, which describes the use of SMTP communication over TLS, is a good example of link-encryption (as described above) which can be implemented to eliminate disclosure of routing information and resulting inference or disclosure.

The limitations of SMTP are very well known. Both delays and message size limitations are common complaints about the SMTP system. With appropriate configuration both of these issues can be addressed. Large messages such as those created during medical imaging, may need to be broken up and sent in multiple parts then reassembled upon reaching the destination. Placing boundaries on delivery time as part of a written standard is necessary while infrastructure BKMs (best known methods) serve as enabling tools which can ensure that implementations meet the published requirements.

For the small and medium sized organizations SMTP will provide the most accessible and trouble-free solution. SOAP and REST will continue to be used and are likely to be considered the transport of choice for the largest and most capable organizations.

Message Confirmation of Receipt

Acknowledgements or Negative-Acknowledgements should be sent for all messages. If there is value in sending a message then there is value in knowing if it has been successfully received.

Confirmation of message delivery is common in the industry. Frequently with SOAP and RESTful implementations successful delivery is assumed from the ‘200 OK’ response message which accompanies an HTTP request. The best implementation is to provide cryptographic Non-Repudiation of Receipt (NRR) for the sent message. NRR refers to an implementation method whereby the sender of a message obtains undeniable proof that the recipient received the message and that the message was not altered in transit. This acknowledgment typically contains the digital signature of the message and the acknowledgment is digitally signed by the receiver of the message. NRRs are quite small, easy to compute and provide more than simple confirmation that the message has been received. Proof that the message was received, by whom, and that it was indeed intact is valuable for both parties in the exchange.

Once an acknowledgement system has been implemented, the additional overhead of NRRs is minimal. ***NRRs are an essential part of any robust acknowledgement solution.***

Additional Questions / Answers

What factors affected your decision to implement P2P messaging as you did?

In the late 1990s Intel implemented its first *modern* P2P messaging system.

The primary reasons for this implementation were to eliminate errors and delays caused by the existing manual processes.

The system was built on the FTP transport but included end-to-end encryption and end-to-end digital signatures for authentication and integrity. This system was proprietary having been built prior to the time when many standards in this space were established. It included FTP for reliable delivery of large files and in retrospect was very much like AS3 (Applicability Statement 3), a draft specification from the IETF. This early system included an acknowledgement which contained a Non-Repudiation of Receipt.

Largely due to its simplicity the system serviced hundreds of customers reliably for several years. It was ultimately replaced by newer standards based systems.

Would you make the same decision if you were designing it today?

Two primary issues kept Intel's early system from growing to thousands of nodes instead of just hundreds.

The first reason was the lack of transport standards. Because the system used proprietary client-server architecture, deployment was quick and easy. This benefit was later negated by the fact that multiple proprietary solutions had to be deployed. ***Standards have immeasurable benefits when they demand simplicity and uniformity.*** Standards which are complex and overly flexible result in costly inoperability and a high level of variability from implementation to implementation.

Our solution would have certainly benefitted from standards which appeared some years later such as AS1 and AS2. This would have allowed us and our trading partners to have a single system to communicate with others instead of unique configurations or even entire systems dedicated to a single end point.

The second limiting factor in this early implementation was just a level above the protected transport level and it had even further reaching ramifications. Data format specifications promise ease of integration until the first trading partner asks for the simplest of exceptions. Often there is a very valid and justifiable reason for this request. Such reasons can include legacy system limitations of field length, character set and timing limitations due to batch processing. Engineers, in an attempt to be accommodating yield to such requests and begin a downward spiral which ultimately leads to a system for which maintenance is difficult, support is complex and upgrades are nearly impossible.

It is very important that information exchange partners make every effort to agree first that standards are of key importance and second that they will both adhere to these standards. Without such an agreement leading an implementation, each deployment results in more and more technical-debt. Ultimately this technical-debt leads to a condition where the cost of maintenance outweighs its benefits relative to the competition and dramatic steps must be taken to rectify the situation.

Extensive experience in this space has led Intel to design and produce a product called SOA-Expressway. SOA-Expressway creates a platform that supports the delivery of PHI between trusted network interfaces. Trust, security and encryption are embedded between router interfaces *in the network,* as opposed to residing within endpoint servers or applications. This enables wire-speed security & governance for P2P authentication/authorization, payload encryption and audit-logging in Healthcare networks.

What do you consider essential requirements for simple, P2P exchanges between two provider organizations?

1. Build the solution on standards; reuse as many existing standards as possible. When writing a new standard, avoid speculative generalization and unnecessary flexibility.
2. Use PKI-based digital signatures for message integrity, authentication and non-repudiation of receipt.
3. Use SMTP for small and medium sized organizations. Combine SMTP with other standards as needed (S/MIME, SMTP over TLS).
4. Protect data at-rest and in-transit using strong standard encryption technology accessible by the widest range of platforms possible.

Do you exchange information with any federal organizations using the NHIN CONNECT gateway? If so, how is that accomplished?

As a provider of industry leading silicon technologies, Intel is not in a role to exchange information with any federal organization using the NHIN CONNECT gateway. However, Intel has supported industry collaboration initiatives around NHIN CONNECT, participating with the University of Virginia at HIMSS 2010 to demonstrate the continuity of care to the home through an NHIN CONNECT data exchange. In addition, our security based technologies are supporting the running of NHIN Connect and the exchange of clinical data within federal healthcare provider organizations. Intel Advanced Encryption Standards-New Instruction and Intel Trusted Execution Technologies are supporting server infrastructures powering these federal agency environments.

Summary: Overcoming the Perception Gap

We have tried to summarize in the previous pages some of the key standards, technologies, and implementation experiences Intel has had with secure, internet-based data exchange for healthcare and other industries. But beyond all of these details and acronyms lies a larger issue that we believe ONC could and should address: namely, the "perception gap" around securing Personal Health Information. This is the gap between the reality of securing health data (it is affordable, achievable, and scalable) and the perception by many healthcare practitioners and even consumers that such security is impossible (it is expensive, impractical, and complex).

In a recent Intel workshop with healthcare CIOs and CTOs—arguably the people who are most tech-savvy and sensitive to the issues of today's Standards hearing of any other stakeholders in healthcare—the panicked perceptions around the HITECH Act and Breach Notification were running wild and rampant. On the one hand, it is good for our industry—indeed, our culture—to take the security of patient data seriously. On the other hand, if the fears about security breaches trump common sense, patient centeredness, and good IT practices, we risk *decreasing* data exchange amongst providers, not increasing it.

We can learn from our past in dealing with this challenge. Since HIPAA was passed in 1996, we at Intel have worked with literally hundreds of healthcare customers whose perceptions of—and responses to—HIPAA were all over the map. We saw small physician practices refusing to fax copies of paper records out of fear of potential HIPAA violations. We saw hospitals creating so much hassle and complexity for password login and credentialing of their authorized physicians and other medical professionals that workflow sometimes came to a halt. And, time and time again, we saw patients unable to get access to their own records because of the impediments, procedures, and gates that some healthcare entities put into place out of an unwarranted and uninformed reaction to HIPAA. The problem was not with the actual statue but with the misinterpretations and overreactions that it generated.

So, too, the breach notification aspects of the HITECH Act could have a similarly paralyzing set of unintended consequences. In our ethnographic studies of EHR adoption and in our healthcare customer engagements, we are already seeing some of that fear, uncertainty, and doubt, especially amongst smaller physician and healthcare practices who do not have a CIO or "IT specialist" or anyone who can translate these standards and technologies. Thus, to the degree that this committee and the ONC in general can help anticipate and mitigate this perception gap, we recommend that you tackle it head on. Providing use case and implementation guidelines to different kinds and sizes of healthcare practices on the steps for doing secure data exchange will be critical. Using Regional Extension Centers and other mechanisms to help integrate these technologies into workflow and clinical practice (if clinicians turn off their hard disk encryption software at the start of each shift then the rest of the data exchange process is already in trouble!) would help to scale out these solutions. And finally, getting the message out that there are viable, valuable solutions for doing secure, internet-based health data exchange will go a long way towards getting everyone to take those first steps on the journey of creating a 21st century healthcare system for all.

[i] See http://www2.standardandpoors.com/spf/pdf/media/global_aging_100710.pdf.